

EXHIBIT A

AO 106 (SDNY Rev. 01/17) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

18 MAG 8377

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

See Attachment A

Case No. S1 17 Cr. 548 (PAC)

APPLICATION FOR A SEARCH AND SEIZURE WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

located in the Southern District of New York, there is now concealed (identify the person or describe the property to be seized):

See Attached Affidavit and its Attachment A

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- evidence of a crime;
- contraband, fruits of crime, or other items illegally possessed;
- property designed for use, intended for use, or used in committing a crime;
- a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section(s)

Offense Description(s)

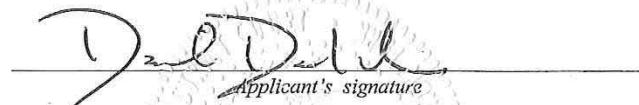
18 U.S.C. §§ 401; 793; 1030; Contempt of court; unlawful disclosure of classified information; unauthorized computer access; wire fraud; obstruction of justice; smuggling contraband into prison; illegal acts related to child pornography.

The application is based on these facts:

See Attached Affidavit and its Attachment A

Continued on the attached sheet.

Delayed notice of 30 days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

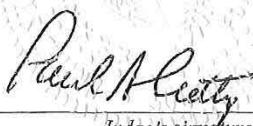
Jeffrey David Donaldson, FBI Special Agent

Printed name and title

Sworn to before me and signed in my presence.

10/02/2018
Date: 10/02/2018

City and state: New York, NY



Judge's signature

The Honorable Paul A. Crotty, U.S.D.J.

Printed name and title

18 MAG 8377

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In the Matter of the Application of the United States of America for a Search Warrant for the Premises Known and Described as 7 South Unit, 7 North Unit, Including the Cells Located In Those Units, and the Education Department's Law Library on the Second Floor, located in Metropolitan Correctional Center, 150 Park Row, New York, New York 10007, as well as Any Closed Containers/Items Contained in the Premises

SOUTHERN DISTRICT OF NEW YORK) ss.:

JEFF D. DONALDSON, being duly sworn, deposes and says:

I. Introduction

A. Affiant

1. I am a Special Agent of the Federal Bureau of Investigation ("FBI") assigned to the New York Field Office, and have been employed by the FBI since 2010. I am currently assigned to a squad responsible for counterespionage matters and have worked in the field of counterintelligence from 2010 to present. In the course of my duties as a Special Agent, I am responsible for investigating offenses involving espionage and related violations of law, including unauthorized retention, gathering, transmitting or losing classified documents or materials; unauthorized removal and retention of classified documents or materials; illegally acting in the United States as a foreign agent; other national security offenses; and the making of false statements. As a result of my involvement in espionage investigations and investigations involving the unauthorized disclosure or retention of classified information, as well as my training in counterintelligence operations, I am familiar with the tactics, methods, and techniques of United States persons who possess, or have possessed a United States Government security clearance and

may choose to harm the United States by misusing their access to classified information. I am also familiar, though my training and experience with the use of computers in criminal activity and the forensic analysis of electronically stored information.

2. I make this Affidavit in support of an application pursuant to Rule 41 of the Federal Rules of Criminal Procedure for a second warrant to search the premises specified below (the "Subject Premises") for the items and information described in Attachment A. This Affidavit is based upon my personal knowledge; my review of documents and other evidence; my conversations with other law enforcement personnel; and my training, experience and advice received concerning the use of computers in criminal activity and the forensic analysis of electronically stored information ("ESI"). Because this Affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

B. The Subject Premises

3. The Subject Premises is particularly described as the 7 South Unit ("Unit-1"), 7 North Unit ("Unit-2"), including the cells located in those units, and the Education Department's law library on the second floor (the "Law Library," together with "Unit-1" and "Unit-2," the "Subject Premises") located in Metropolitan Correctional Center, 150 Park Row, New York, New York 10007.

C. The Subject Offenses

4. For the reasons detailed below, I believe that there is probable cause that the Subject Premises contain evidence, fruits, and instrumentalities of Title 18, United States Code, Sections 401 (contempt of court), 793 (unlawful disclosure of classified information); 1030 (unauthorized

computer access), 1343 (wire fraud), 1503 (obstruction of justice), 1791 (smuggling contraband into a federal detention facility) and 2252A (illegal acts related to child pornography); as well as conspiracies and attempts to violate these provisions and aiding and abetting these offenses, among other statutes (the “Subject Offenses”).

D. Terminology

5. The term “computer,” as used herein, is defined as set forth in 18 U.S.C. § 1030(e)(1).

6. The terms “records,” “documents,” and “materials” include all information recorded in any form, visual or oral, and by any means, whether in handmade form (including, but not limited to, writings, drawings, paintings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical discs, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device), as well as the equipment needed to record such information (including but not limited to cameras and video recording and storage devices).

II. Probable Cause and Request to Search

A. Overview

7. As described in further detail below, through this application, the Government seeks a warrant to search the Subject Premises for two iPhones one with IMEI 358793052665161 and one with IMEI 354444064445994 (the “Contraband iPhones”); a Samsung cellphone with

IMEI number 357073084445432 and/or Serial Number R58J61Q0JCD (the “Schulte Cellphone,” together with the Contraband iPhones, the “Contraband Cellphones”); and copies of certain documents written by Joshua Adam Schulte (the “Schulte Documents”).¹ Schulte—who has been indicted for, among other things, possession of child pornography and unlawful disclosure of classified information—and another inmate, Omar Amanat—who was convicted at trial of various forms of fraud, including securities fraud—have been using the Contraband Cellphones that were smuggled into the MCC to, among other things, fabricate evidence and disseminate information that is either protected by a court-entered protective order or that is classified.

B. Background on Amanat and Schulte’s Detention at the MCC

8. Based on my training and experience, my participation in this investigation, and my conversations with other law enforcement agents and others, and my review of reports prepared by others, including other FBI agents, I have learned, among other things, that:

- a. Between in or about 2012 and November 2016, Schulte was employed by the Central Intelligence Agency (the “CIA”).
- b. At the CIA, Schulte worked at a specific group (the “CIA Group”) that, among other things, developed computer applications that the CIA used to gather intelligence abroad.
- c. As part of his work, Schulte developed specialized skills in, among other things, hacking computers and computer networks and secretly obtaining data from computers and computer networks.
- d. In or about November 2016, Schulte resigned from the CIA. Prior to his resignation, Schulte had disclosed to other CIA employees that he was angry at what he perceived

¹ One of the Contraband iPhones was seized by the MCC on or about September 26, 2018.

to be his mistreatment by CIA management in connection with a dispute Schulte had had with another CIA employee.

e. Beginning on or about March 7, 2017 through in or about November 2017, the website wikileaks.org (“WikiLeaks”) published information from the CIA Group at which Schulte previously worked (the “Leak”). The Leak appears to be the largest unauthorized public disclosure of CIA information in the history of the agency.

f. On or about August 24, 2017, the FBI arrested Schulte for, among other things, possession of child pornography, based on, in part, the FBI’s discovery of approximately 10,000 images of apparent child pornography on a personal desktop computer used by Schulte.

g. Schulte was initially released on bail on or about September 15, 2017, over the Government’s objection. Schulte’s bail was revoked, however, in connection with his violation of his bail conditions, in particular, restrictions on his use of computers or the Internet. Schulte’s actions included, among other things, using an online network that allows for anonymous browsing of the Internet. Schulte has been detained at the MCC since on or about December 14, 2017.

h. On or about June 18, 2018, the Government filed a superseding indictment that, in addition to containing the original child pornography charges, also charged Schulte with violations of, among other statutes, Title 18, United States Code, Sections 793 and 1030, in connection with the Leak.

i. The Government has produced to Schulte certain search warrant affidavits (the “Schulte Search Warrant Affidavits”) pursuant to a protective order entered by the Court on or about September 18, 2017 (the “Schulte Protective Order”). Based on the terms of the protective order, Schulte and his defense team were not permitted to disclose the Schulte Search Warrant

Affidavits or the information contained in them to anyone not involved in the preparation of Schulte's defense.

9. Based on my training and experience, my participation in this investigation, my review of reports and other documents prepared by others, and my conversations with other law enforcement agents and others, including an FBI agent involved in an earlier investigation and prosecution of Amanat, I have learned, among other things, that:

a. On or about July 13, 2016, the Government filed a superseding indictment charging Amanat with wire fraud, conspiracy to commit wire fraud, aiding and abetting investment advisor fraud, and conspiracy to commit securities fraud.

b. Amanat was arrested that day and released on bail on or about July 22, 2016.

c. On or about December 26, 2017, Amanat was convicted on all counts after a jury trial before the Honorable Paul G. Gardephe.

d. Amanat has been detained at the MCC since on or about December 26, 2017.

e. Amanat is currently scheduled to be sentenced on or about October 18, 2018 although that sentencing date may be adjourned because of requests by defense counsel for Amanat and his co-defendant, Kaleil Isaza Tuzman, for a *Fatico* hearing. Isaza Tuzman was also convicted on or about December 26, 2017 and is currently on bail pending sentencing.

f. Amanat's brother and co-defendant, Irfan Amanat, is scheduled to proceed to trial before Judge Gardephe on October 22, 2018, on charges of wire fraud, conspiracy to commit wire fraud, aiding and abetting investment advisor fraud, and conspiracy to commit securities fraud.

10. Based on my training and experience, my participation in this investigation, my conversations with other law enforcement agents and others, and my review of reports and recorded telephone conversations, I have learned, among other things, that:

- a. Schulte and Amanat are cellmates at the MCC, and are housed in Unit-1.²
- b. During recorded telephone conversations from the MCC,³ Schulte has stated that he and Amanat are friends and that Schulte is helping Amanat with a report that will help to prove Amanat's alleged innocence.

C. Schulte's Violation of the Schulte Protective Order and Disclosure of Classified Information While at the MCC

11. Based on my training and experience, my conversations with other law enforcement agents and others, my participation in this investigation, and my review of reports and recorded conversations, I have learned, among other things, that:

a. In or about April 2018, in recorded calls from the MCC, Schulte discussed with members of his family his desire to talk to members of the media about his case. Schulte also indicated that he had written several documents, which he called "articles," that discussed his case (the "Schulte Articles") and which he wanted to be disseminated to the media. It appears from the calls that at least some of the Schulte Articles may have been provided to one or more members of the media.

b. In or about April 2018, in a recorded call from the MCC, Schulte spoke with an individual who appeared to be a member of the media. During the call, Schulte discussed the information contained in one of the Schulte Search Warrant Affidavits and why he felt that

² I understand that based on some of the conduct described in this Affidavit, MCC officials may move Schulte to another part of the MCC so that he is no longer Amanat's cellmate.

³ All conversations or documents referenced in this Affidavit are described in substance and in part.

information was inaccurate. When asked if the information he was discussing was classified, Schulte responded that it was not classified, but that it was protected by the “protective order.” Nevertheless, Schulte continued to disclose information found in one of the Schulte Search Warrant Affidavits.

c. On or about May 15, 2018, the *Washington Post* and the *New York Times* published articles about Schulte’s case, in which they indicated that their reporters had learned of information contained in at least one of the Schulte Search Warrant Affidavits.

d. On or about May 21, 2018, at the Government’s request, the Court held a conference to address Schulte’s violation of the Schulte Protective Order. During the hearing, the Government noted, among other things, that it had reviewed recordings of calls Schulte had participated in from the MCC.

e. On or about June 20, 2018, at his arraignment on the superseding indictment, Schulte submitted a handwritten pro se bail motion to the Court (the “Pro Se Bail Motion,” ~~together with the Schulte Articles, the “Schulte Documents.”~~⁴) *500*

f. The day after Schulte submitted the Pro Se Bail Motion, the Government informed Schulte’s counsel that the Pro Se Bail Motion was undergoing a review by the CIA to determine whether it contained classified information.

g. It appears that after the Government informed Schulte’s counsel about the classification review, Schulte may have sent the Pro Se Bail Motion to an attorney and his parents.

h. The CIA has reviewed the Pro Se Bail Motion and the Schulte Articles, and has determined that the Pro Se Bail Motion and at least one of the Schulte Articles contain classified information.

⁴ The Schulte Documents are more particularly described in Attachment A, *and include only the Schulte Articles.* *500*

D. Amanat's Fabrication of Evidence During His Trial

12. Based on my training and experience, my participation in this investigation, and my conversations with other law enforcement agents and others, including an FBI agent involved in a prior investigation and prosecution of Amanat, I have learned, among other things, the following:

a. During his trial, Amanat sought to introduce, among other things, approximately five emails (the "Amanat Fabricated Emails"), four of which were admitted initially several in redacted form.

b. In response, during two hearings held outside the presence of the jury as well as in a rebuttal case before the jury, the Government submitted evidence showing that the Amanat Fabricated Emails had been faked by Amanat, including, among other things:

i. Evidence of discrepancies in header information, including time stamps associated with the Amanat Fabricated Emails and other emails introduced at trial.

ii. Evidence that certain of the Amanat Fabricated Emails were not found in certain email accounts or on electronic media used by the purported recipients of the emails.

iii. Evidence that the Amanat Fabricated Emails were inconsistent with other contemporaneous and inculpatory communications involving Amanat.

iv. An email communication between Amanat and his brother and co-defendant, Irfan Amanat, concerning how to delete emails from a certain email account.

v. Expert testimony from an experienced FBI Special Agent assigned to a cyber squad that four of the five Amanat Fabricated Emails were fake and/or were not sent on the date and time on which they appeared to have been sent.

c. As noted above, Amanat was convicted by the jury of all counts.

E. Schulte and Amanat Arrange to have Cellphones Smuggled into the MCC

13. I have participated in an interview of an inmate at the MCC who was housed in Unit-1 with Amanat and Schulte until recently (the “CS”).⁵ During that interview, the CS reported that, among other things:

a. For the past several months, the CS has been paid by Amanat to store and charge the Contraband Cellphones.

b. The Contraband Cellphones were smuggled into the MCC and protected from detection through a network of visitors to the facility, inmates, and correctional officers.

c. For a time, the CS was tasked with storing and charging the Contraband Cellphones in the CS’s cell. During that time-period, the CS also knew the passwords for the devices.

d. At some point, Schulte decided that he no longer wanted the CS to know the password for the Schulte Cellphone or to store it. Since around that time, the Schulte Cellphone has been stored in other inmates’ cells.

e. Schulte told the CS that Schulte had implemented certain security protocols with respect to the Schulte Cellphone, such as changing the cellphone’s unique device identifier and enabling a function by which all the data on the Schulte Cellphone would be deleted if someone other than Schulte tried to access the phone.

f. Prior to Schulte’s retrieval of the Schulte Cellphone, the CS would regularly take screenshots of messages and recorded videos involving the Contraband Cellphones. The CS

⁵ The CS is facing immigration and narcotics trafficking charges, and is cooperating in the hope of receiving a more lenient sentence and potentially immigration benefits. As described in this Affidavit, the CS’s information has been at least partly corroborated by, among other things, a seizure of at least one contraband cellphone.

subsequently stored those screenshots in an email account the CS created (the “CS Account”). Based on these messages and the CS’s conversations with Schulte and Amanat, the CS understood that, among other things:

i. Schulte and Amanat were using the Contraband Cellphones in connection with the creation of some sort of report that would be submitted to Amanat’s sentencing judge (Judge Gardephe) to show that the Amanat Fabricated Emails were allegedly real.

ii. The CS also recalled a communication over at least one of the Contraband Cellphones relating to “Vault 7,” which is the name used by WikiLeaks for the Leak.

g. Amanat and Schulte also discussed their need to have the Contraband Cellphones with them when they accessed discovery at the Law Library.

h. During the interview, the CS consented to the search of the CS Account, and provided not only the name of the CS Account, but also the password for it.

14. Based on my participation in this investigation, conversations with other participants in the investigation, and my review of reports prepared during the investigation, I have learned, among other things, that:

a. Unit-1 and Unit-2 are on the same floor of the MCC and are connected by a corridor.

b. Although inmates from the two units are prohibited from interacting with each other in the corridor between Unit-1 and Unit-2, inmates are, at times, able to meet briefly in that space.

c. On or about on or about September 26, 2018, MCC officials recovered one of the Contraband iPhones from Unit-1. It does not appear, however, that the other Contraband Cellphones have been recovered by MCC officials yet.

d. The search for the other Contraband Cellphones is ongoing, and has included, among other things, searching multiple cells in Unit-1, including Schulte and Amanat's cell, and cells in proximity to their cell.

F. Evidence of Schulte's and Amanat's Illegal Activity Using the Contraband Cellphones

15. Based on my review of the CS Account, my participation in this investigation, conversations with other participants in the investigation, and my review of reports prepared during the investigation, I have learned, among other things, that:

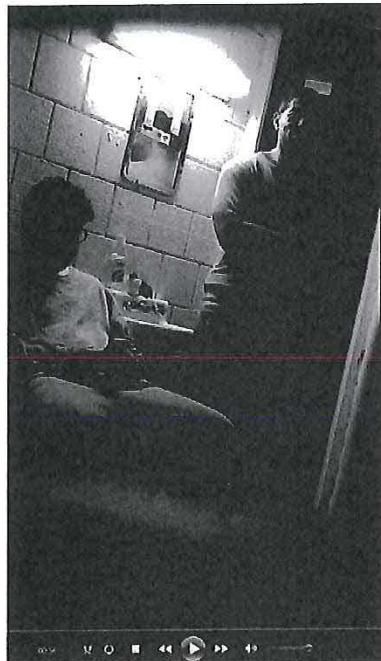
a. The CS Account contains approximately 450 electronic files (including videos and photographs) of the Contraband Cellphones. These files include, among other things, video recordings of Schulte and Amanat using the Contraband Cellphones and screenshots (or images) of communications received and/or sent using the Contraband Cellphones in connection with Schulte's and Amanat's intended fabrication of evidence and/or dissemination of materials protected by the Protective Order or that appear classified, including the Schulte Documents.

b. Below are several still images taken from videos retrieved from the CS Account that show Schulte and Amanat using the Contraband Cellphones in the MCC:

Video 1 (Image 1)



Video 2 (Image 1)

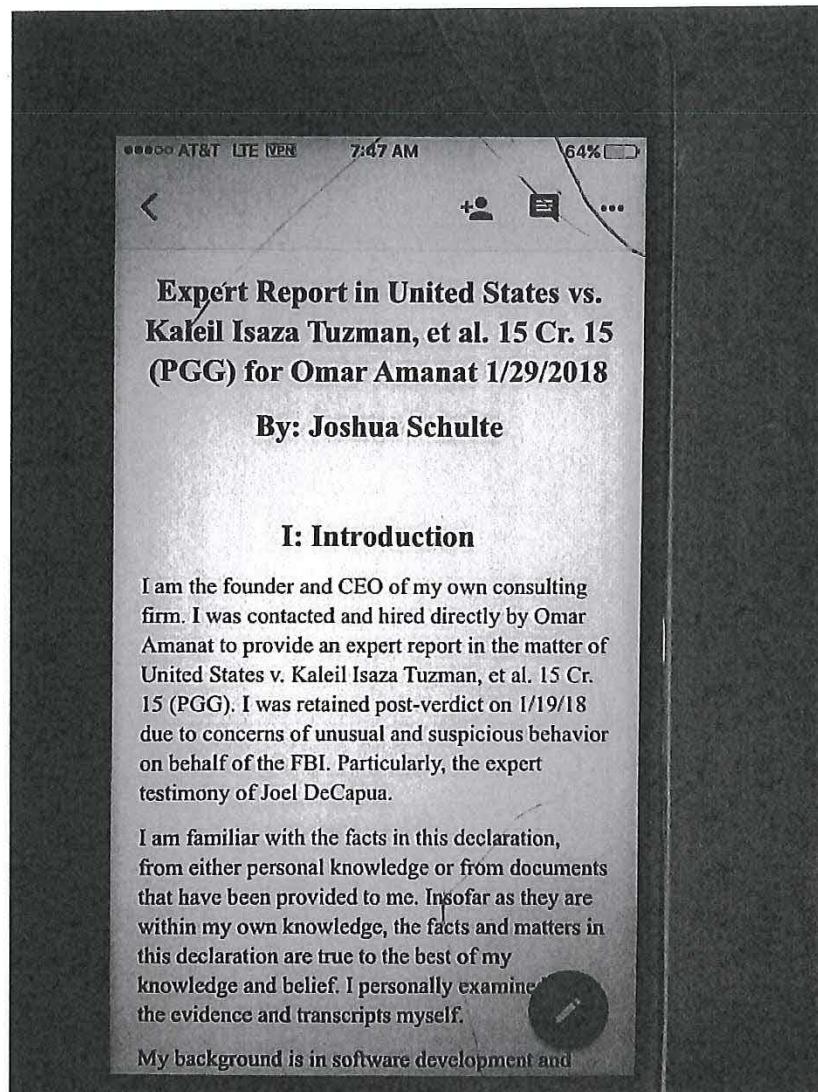


Video 2 (Image 2)

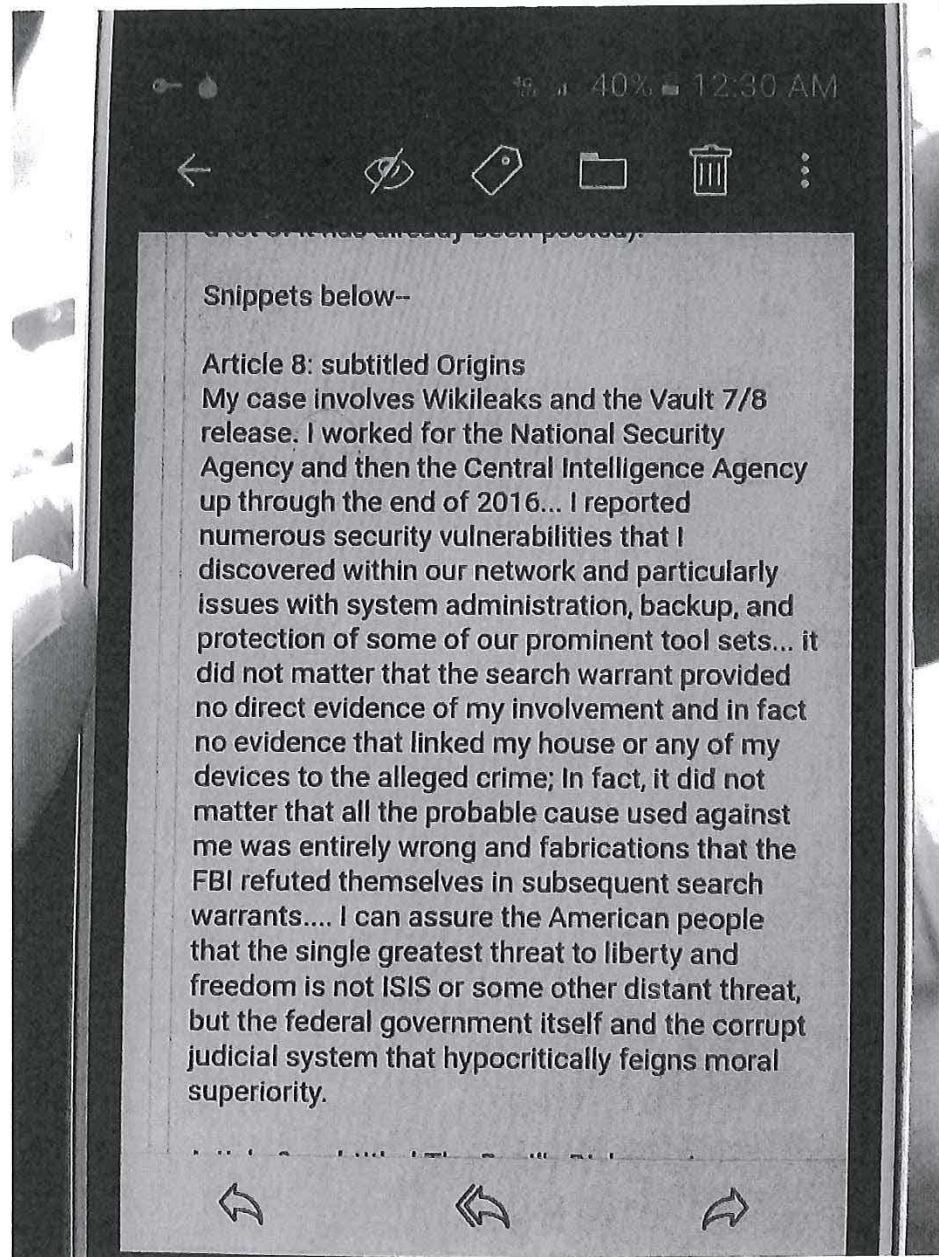


c. Below are images from the CS Account reflecting communications using the Contraband Cellphones:

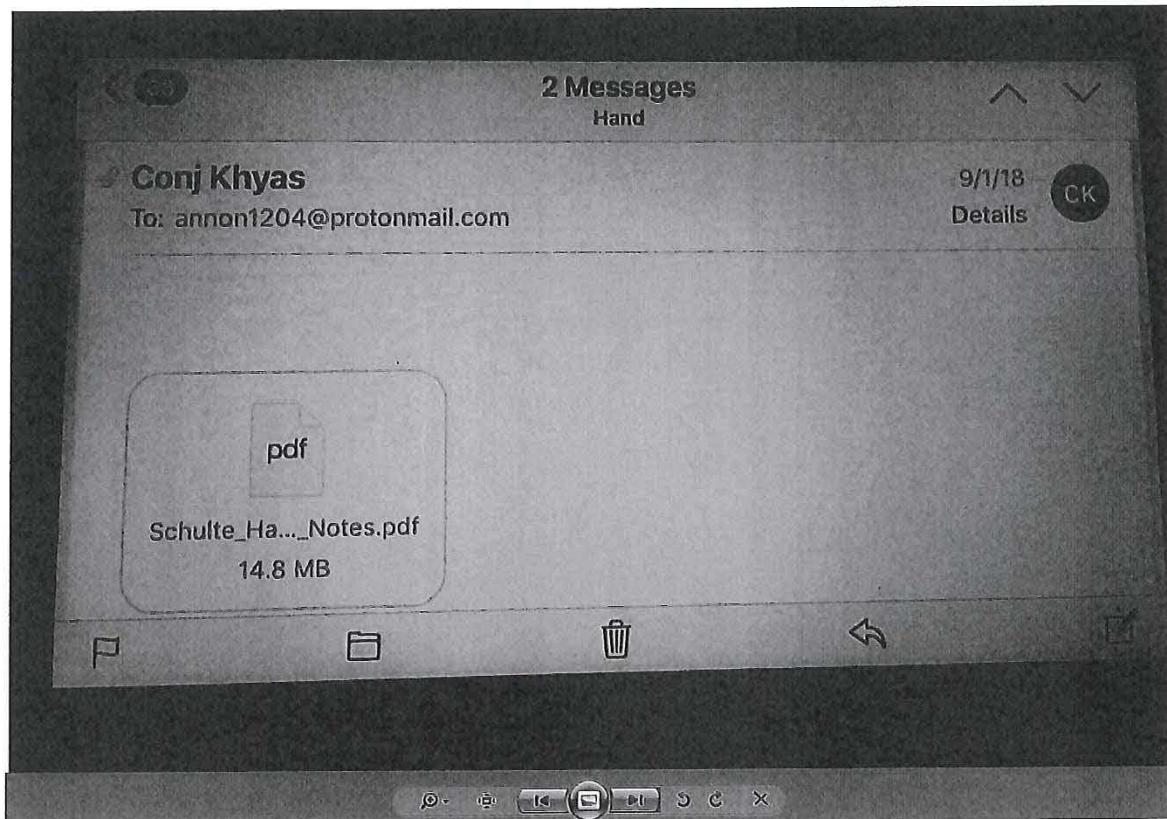
i. The image below from one of the Contraband Cellphones appears to be a draft report prepared by Schulte and Amanat related to the fabricated emails from Amanat's trial.



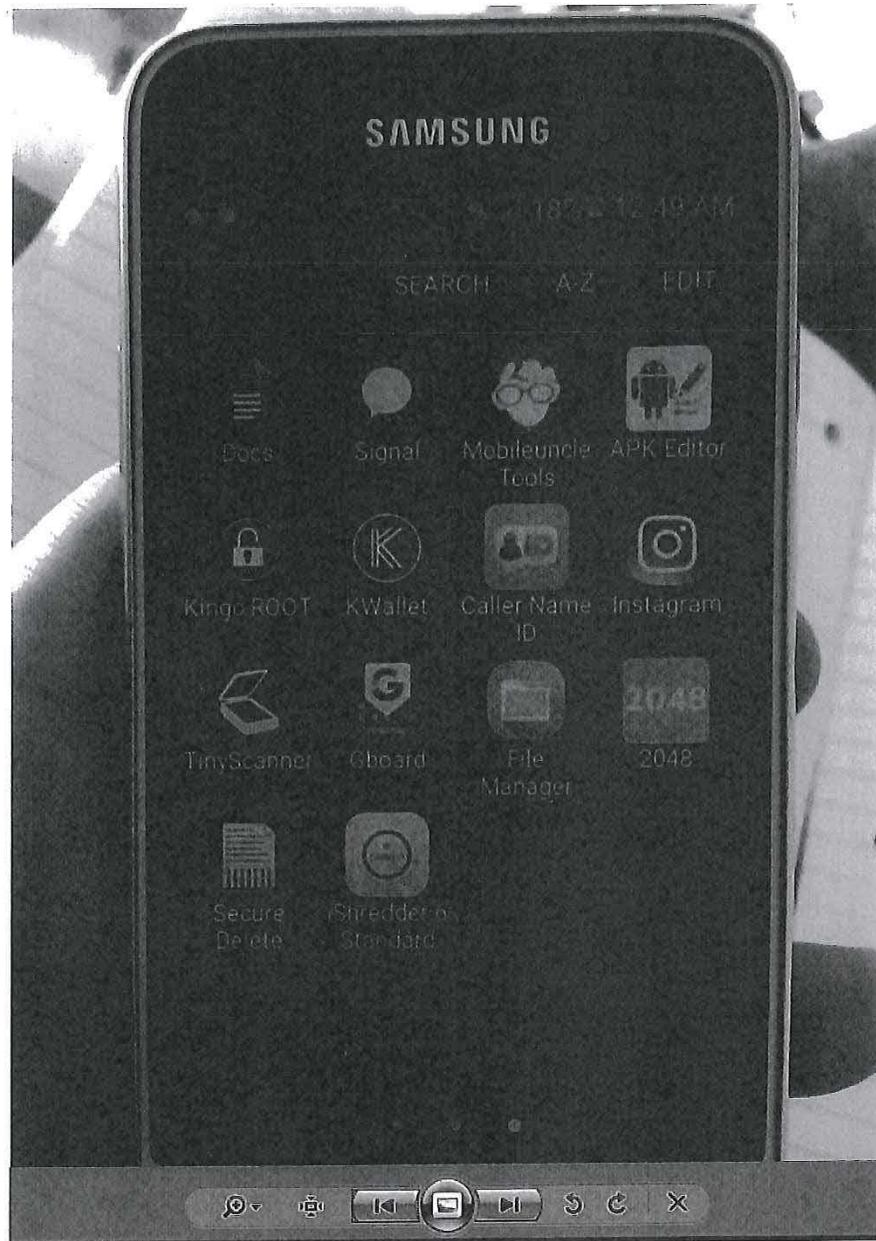
ii. The image below from one of the Contraband Cellphones appears to be an email describing an excerpt from one of the Schulte Articles:



iii. The image below is a screenshot of what appears to be an email sent over one of the Contraband Cellphones. "Protonmail" is an encrypted email service based abroad, and the file "Schulte_Ha..._Notes.pdf" appears to be a reference to the information contained in the Pro Se Bail Motion.



iv. The image below is a screenshot of one of the Contraband Cellphones that depicts certain applications that have been downloaded to the phone, including “Secure Delete” and “IShredder”:



G. Probable Cause Justifying Search of ESI

16. Based on the foregoing, and based on my training and experience, I know that Amanat and Schulte have used (or are using) the Contraband Cellphones to, among other things, create documents and communicate with others outside the MCC. Moreover, like individuals engaged in any other kind of activity, individuals who engage in the Subject Offenses store records relating to their illegal activity and to persons involved with them in that activity on electronic devices such as the Contraband Cellphones. Such records can include, for example logs of online “chats” with co-conspirators; email correspondence; contact information of co-conspirators, including telephone numbers, email addresses, and identifiers for instant messaging and social medial accounts; stolen financial and personal identification data, including bank account numbers, credit card numbers, and names, addresses, telephone numbers, and social security numbers of other individuals; and/or records of illegal transactions using stolen financial and personal identification data. Individuals engaged in criminal activity often store such records in order to, among other things, (1) keep track of co-conspirators’ contact information; (2) keep a record of illegal transactions for future reference; (3) keep an accounting of illegal proceeds for purposes of, among other things, dividing those proceeds with co-conspirators; and (4) store stolen data for future exploitation.

17. As a result, there is probable cause to believe that the Contraband Cellphones contain some or all of the following:

- a. The phone numbers associated with the Contraband Cellphones, as well as call log information of phone numbers of incoming and outgoing, and missed or unanswered calls to and from the Contraband Cellphones;
- b. Address books and contact lists stored on the Contraband Cellphones or its memory card(s);

c. Voicemail messages, opened or unopened, related to the Subject Offenses;

d. Evidence concerning the identity or location of the owner(s) or user(s) of the Contraband Cellphones;

e. Evidence concerning the identity and/or location of the individual(s) involved in the commission of the Subject Offenses;

f. Evidence of communications among, or concerning, participants in or witnesses to the commission of the Subject Offenses;

g. Contact information of co-conspirators and witnesses to the commission of the Subject Offenses, including telephone numbers, email addresses, and identifiers for instant messaging and social media accounts;

h. Text, data, "chats," MMS ("Multimedia Messaging Service") messages, SMS ("Short Message Service") messages, FaceTime messages, and e-mail messages, any attachments to those messages, such as digital photographs and videos, and any associated information, such as the phone number or e-mail address from which the message was sent, pertaining to the Subject Offenses;

i. Digital photographs and videos related to the Subject Offenses;

j. Browsing history, websites visited, and internet searches conducted on the Contraband Cellphones related to the Subject Offenses.

18. Based on my training and experience, I also know that, where computers are used in furtherance of criminal activity, evidence of the criminal activity can often be found months or even years after it occurred. This is typically true because:

- Electronic files can be stored on a hard drive for years at little or no cost and users thus have little incentive to delete data that may be useful to consult in the future.

- Even when a user does choose to delete data, the data can often be recovered months or years later with the appropriate forensic tools. When a file is “deleted” on a home computer, the data contained in the file does not actually disappear, but instead remains on the hard drive, in “slack space,” until it is overwritten by new data that cannot be stored elsewhere on the computer. Similarly, files that have been viewed on the Internet are generally downloaded into a temporary Internet directory or “cache,” which is only overwritten as the “cache” fills up and is replaced with more recently viewed Internet pages. Thus, the ability to retrieve from a hard drive or other electronic storage media depends less on when the file was created or viewed than on a particular user’s operating system, storage capacity, and computer habits.
- In the event that a user changes computers, the user will typically transfer files from the old computer to the new computer, so as not to lose data. In addition, users often keep backups of their data on electronic storage media such as thumb drives, flash memory cards, CD-ROMs, or portable hard drives.

19. Based on the foregoing, I respectfully submit there is probable cause to believe that Schulte and Amanat are engaged in the Subject Offenses, and that evidence of this criminal activity is likely to be found in the Subject Premises and on the Contraband Cellphones.

III. Procedures for Searching ESI

A. Execution of Warrant for ESI

20. Federal Rule of Criminal Procedure 41(e)(2)(B) provides that a warrant to search for and seize property “may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information . . . for later review.” Consistent with Rule 41, this application requests authorization to seize any computer devices and storage media and transport them to an appropriate law enforcement facility for review. This is typically necessary for a number of reasons:

- First, the volume of data on computer devices and storage media is often impractical for law enforcement personnel to review in its entirety at the search location.
- Second, because computer data is particularly vulnerable to inadvertent or intentional modification or destruction, computer devices are ideally examined in a controlled environment, such as a law enforcement laboratory, where trained personnel, using specialized software, can make a forensic copy of the storage media that can be subsequently reviewed in a manner that does not change the underlying data.

- Third, there are so many types of computer hardware and software in use today that it can be impossible to bring to the search site all of the necessary technical manuals and specialized personnel and equipment potentially required to safely access the underlying computer data.
- Fourth, many factors can complicate and prolong recovery of data from a computer device, including the increasingly common use of passwords, encryption, or other features or configurations designed to protect or conceal data on the computer, which often take considerable time and resources for forensic personnel to detect and resolve.

B. Review of ESI

21. Following seizure of any cellphones and/or the creation of forensic image copies, law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) will review the ESI contained therein for information responsive to the warrant.

22. In conducting this review, law enforcement personnel may use various techniques to determine which files or other ESI contain evidence or fruits of the Subject Offenses. Such techniques may include, for example:

- surveying directories or folders and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- conducting a file-by-file review by “opening” or reading the first few “pages” of such files in order to determine their precise contents (analogous to performing a cursory examination of each document in a file cabinet to determine its relevance);
- “scanning” storage areas to discover and possibly recover recently deleted data or deliberately hidden files; and
- performing electronic keyword searches through all electronic storage areas to determine the existence and location of data potentially related to the subject matter of the investigation⁶; and

⁶ Keyword searches alone are typically inadequate to detect all relevant data. For one thing, keyword searches work only for text data, yet many types of files, such as images and videos, do not store data as searchable text. Moreover, even as to text data, there may be information properly

- reviewing metadata, system information, configuration files, registry data, and any other information reflecting how, when, and by whom the computer was used.

23. Law enforcement personnel will make reasonable efforts to restrict their search to data falling within the categories of evidence specified in the warrant. Depending on the circumstances, however, law enforcement personnel may need to conduct a complete review of all the ESI from seized devices or storage media to evaluate its contents and to locate all data responsive to the warrant.

C. Return of ESI

24. If the Government determines that the electronic devices are no longer necessary to retrieve and preserve the data, and the devices themselves are not subject to seizure pursuant to Federal Rule of Criminal Procedure 41(c), the Government will return these items, upon request. Computer data that is encrypted or unreadable will not be returned unless law enforcement personnel have determined that the data is not (i) an instrumentality of the offense, (ii) a fruit of the criminal activity, (iii) contraband, (iv) otherwise unlawfully possessed, or (v) evidence of the Subject Offenses.

subject to seizure but that is not captured by a keyword search because the information does not contain the keywords being searched.

IV. Conclusion and Ancillary Provisions

25. Based on the foregoing, I respectfully request the court to issue a warrant to search and seize the items and information specified in Attachment A to this Affidavit and to the Search and Seizure Warrant.

26. In light of the confidential nature of the continuing investigation, I respectfully request that this Affidavit be maintained under seal until the Court orders otherwise.



JEFF D. DONALDSON
Special Agent
Federal Bureau of Investigation

Sworn to before me on
this 1st day of October 2018
2nd



THE HONORABLE PAUL A. CROTTY
UNITED STATES DISTRICT JUDGE
SOUTHERN DISTRICT OF NEW YORK

Attachment A

I. Premises to be Searched—Subject Premises

The premises to be searched (the “Subject Premises”) is described as follows, and includes all locked and closed containers found therein:

The Subject Premises is particularly described as the 7 South Unit, 7 North Unit, including the cells located in those units, and the Education Department’s law library on the second floor of the building, located in Metropolitan Correctional Center, 150 Park Row, New York, New York 10007.

II. Execution of the Warrant

Law enforcement agents are permitted to execute the search warrant at any time in the day or night. Upon the execution of this warrant, notice will be provided at or as soon as possible after the execution of the search.

III. Items to Be Searched and Seized

A. Evidence, Fruits, and Instrumentalities of the Subject Offenses

The items to be searched and/or seized from the Subject Premises include the following evidence, fruits, and instrumentalities of: Title 18, United States Code, Sections 401 (contempt of court); Title 18, United States Code, Section 793 (unlawful disclosure of classified information); Title 18, United States Code, Section 1030 (unauthorized computer access), Title 18, United States Code, Section 1343 (wire fraud), Title 18, United States Code, Section 1503 (obstruction of justice), Title 18, United States Code, Section 1791 (smuggling contraband into a federal detention facility) and Title 18, United States Code, Section 2252A (illegal acts related to child pornography); as well as conspiracies and attempts to violate these provisions and aiding and abetting these offenses, among other statutes (the “Subject Offenses”):

1. A Samsung cellphone with IMEI 357073084445432 and/or Serial Number R58J61Q0JCD (the “Schulte Cellphone”).

2. An iPhone cellphone with IMEI 358793052665161 ("iPhone-1");
3. An iPhone cellphone with IMEI 354444064445994 ("iPhone-2," together with iPhone-1 and the Schulte Cellphone, the "Contraband Cellphones").
4. Evidence pertaining to the smuggling in of the Contraband Cellphones.
5. Evidence concerning the identity or location of, and communications with, any co-conspirators.
6. Any and all notes, documents, records, correspondence, or materials, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, other digital data files and web cache information, and handwritten notes), pertaining to the unauthorized retention, gathering, and transmission of classified documents or materials, and the unauthorized removal and retention of classified documents or materials, and, in particular, the documents bearing the following titles or descriptions:
 - a. Article 1: "Presumption of Innocence: A petition for redress of grievances"
 - b. Article 2: "Presumption of Innocence: A loss of citizenship"
 - c. Article 3: "Presumption of Innocence: Do you want to play a game"
 - d. Article 4: "Presumption of Innocence: Detention is not punishment"
 - e. Article 5: "Presumption of Innocence: Innocent until proven Wealthy"
 - f. Article 6: "Presumption of Innocence: Can you afford to be accused?"
 - g. Article 7: "Presumption of Innocence: A proposed solution"
 - h. Article 8: "Presumption of Innocence: Origins"
 - i. Article 9: "... unalienable Rights, that among these are Life, Liberty and the pursuit of Happiness"

j. Handwritten document dated on or about June 7, 2018 and titled "United States v. Joshua Adam Schulte, 17 Cr. 548 (PAC), PRO SE BAIL APPLICATION." 52

7. Evidence of the Subject Offenses on the Contraband Cellphones, including:

a. The phone numbers associated with the Contraband Cellphones, as well as call log information of phone numbers of incoming and outgoing, and missed or unanswered calls to and from the Contraband Cellphones;

b. Address books and contact lists stored on the Contraband Cellphones or its memory card(s);

c. Voicemail messages, opened or unopened, related to the Subject Offenses;

d. Evidence concerning the identity or location of the owner(s) or user(s) of the Contraband Cellphones;

e. Evidence concerning the identity and/or location of the individual(s) involved in the commission of the Subject Offenses;

f. Evidence of communications among, or concerning, participants in or witnesses to the commission of the Subject Offenses;

g. Contact information of co-conspirators and witnesses to the commission of the Subject Offenses, including telephone numbers, email addresses, and identifiers for instant messaging and social media accounts;

h. Text, data, "chats," MMS ("Multimedia Messaging Service") messages, SMS ("Short Message Service") messages, FaceTime messages, and e-mail messages, any attachments to those messages, such as digital photographs and videos, and any associated information, such as the phone number or e-mail address from which the message was sent, pertaining to the Subject Offenses;

i. Digital photographs and videos related to the Subject Offenses;

j. Browsing history, websites visited, and internet searches conducted on the Contraband Cellphones related to the Subject Offenses.

8. If law enforcement personnel seize the Contraband Cellphones, the personnel will search the device within a reasonable amount of time, not to exceed 60 days from the date of execution of the warrant. If, after such a search has been conducted, it is determined that a computer or device contains any data listed in paragraphs 2 and 3, the Government will retain the computer or device. If it is determined that the computer(s) or device(s) are no longer necessary to retrieve and preserve the data, and the items are not subject to seizure pursuant to Federal Rule of Criminal Procedure 41(b), such materials and/or equipment will be returned within a reasonable time. In any event, such materials and/or equipment shall be returned no later than 60 days from the execution of this warrant, unless further application is made to the Court.

B. Search and Seizure of Electronically Stored Information

The items to be searched and seized from the Subject Premises also include any cellphones that may contain any electronically stored information falling within the categories set forth in Section III.A of this Attachment above, including, but not limited to, desktop and laptop computers, disk drives, modems, thumb drives, personal digital assistants, smart phones, digital cameras, and scanners. The items to be searched and seized from the Subject Premises also include:

1. Any items or records needed to access the data stored on any seized or copied computer devices or storage media, including but not limited to any physical keys, encryption devices, or records of login credentials, passwords, private encryption keys, or similar information.

2. Any items or records that may facilitate a forensic examination of the computer devices or storage media, including any hardware or software manuals or other information concerning the configuration of the seized or copied computer devices or storage media.

3. Any evidence concerning the persons with access to, control over, or ownership of the seized or copied computer devices or storage media.

C. Review of ESI

Following seizure of any computer devices and storage media and/or the creation of forensic image copies, law enforcement personnel (including, in addition to law enforcement officers and agents, and depending on the nature of the ESI and the status of the investigation and related proceedings, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained therein for information responsive to the warrant.

In conducting this review, law enforcement personnel may use various techniques, including but not limited to:

- surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- opening or cursorily reading the first few "pages" of such files in order to determine their precise contents;
- scanning storage areas to discover and possibly recover recently deleted files;
- scanning storage areas for deliberately hidden files;

- performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation; and
- making reasonable efforts to utilize computer search methodology to search only for files, documents, or other electronically stored information within the categories identified in this Attachment.